

INPI

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

FR 99 / 2174

09/786616

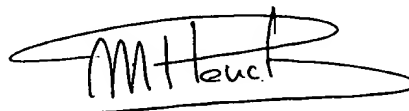
REC'D 27 SEP 1999

WIPO

PCT

BREVET D'INVENTION**CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION****COPIE OFFICIELLE****PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **17 SEP. 1999**Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets**Martine PLANCHE**INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE

26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

11 SEP 1998

N° D'ENREGISTREMENT NATIONAL

98 11327

DÉPARTEMENT DE DÉPÔT

DATE DE DÉPÔT

11 SEP. 1998

1

**NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE**

**Patrick Richard
THOMSON multimedia
46 Quai Alphonse Le Gallo
92648 Boulogne Cedex**

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention

☐ demande divisionnaire

☐ certificat d'utilité

☐ transformation d'une demande
de brevet européen

demande initiale

☐ brevet d'invention

n° du pouvoir permanent

PG 6075

références du correspondant

PF980061

téléphone

0141865565

date

Établissement du rapport de recherche

☐ différé

☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui

☒ non

Titre de l'invention (200 caractères maximum)

**PROCEDE DE CHARGEMENT DE DROITS DE SYSTEME A ACCES CONDITIONNEL ET
DISPOSITIF METTANT EN OEUVRE LE PROCEDE**

3 DEMANDEUR (S)

n° SIREN

code APE-NAF

Norm et prénoms (souligner le nom patronymique) ou dénomination

THOMSON multimedia

Forme juridique

S.A.

Nationalité (s)

Française

Adresse (s) complète (s)

**46 Quai Alphonse Le Gallo
92100 BOULOGNE**

Pays

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui

☒ non

Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois

☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS antérieures à la présente demande

n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire - n° d'inscription)

P. Richard
Patrick Richard

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Petersbourg

75800 Paris Cédex 08

Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

9811327

TITRE DE L'INVENTION :

**PROCEDE DE CHARGEMENT DE DROITS DE SYSTEME A ACCES
CONDITIONNEL ET DISPOSITIF METTANT EN OEUVRE LE
PROCEDE**

LE(S) SOUSSIGNÉ(S)

THOMSON multimedia

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

- GAUCHE Laurent

domicilié à :

**THOMSON multimedia
46 Quai Alphonse Le Gallo
92648 Boulogne Cedex**

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

11 Septembre 1998

Patrick Richard

P. Richard

**PROCEDE DE CHARGEMENT DE DROITS DE SYSTEME
A ACCES CONDITIONNEL ET DISPOSITIF METTANT EN OEUVRE LE
PROCEDE.**

5 La présente invention concerne un système à accès conditionnel et, plus particulièrement, un procédé de chargement des droits qu'un utilisateur peut acquérir pour accéder à un service distribué au sein d'un système à accès conditionnel.

10 Un système à accès conditionnel permet à un prestataire de services de ne fournir ses services qu'aux seuls utilisateurs ayant acquis des droits sur ces services. C'est le cas, par exemple, des systèmes de télévision à péage.

15 Comme cela est connu de l'homme de l'art, le service fourni par un prestataire de services est constitué d'une information embrouillée par des mots de contrôle. Afin de désembrouiller l'information, le prestataire de services fournit à chaque utilisateur les mots de contrôle qui ont servi à embrouiller l'information. De façon à garder secrets les mots de contrôle, ceux-ci sont fournis après avoir été chiffrés avec un algorithme de clé K. Les différents mots de contrôle chiffrés sont envoyés aux différents utilisateurs
20 dans des messages de contrôle communément notés ECM (l'abréviation ECM provient de l'anglais "Entitlement Control Message"). Les mots de contrôle sont déchiffrés dans un processeur sécurisé contenu dans un élément de sécurité tel que, par exemple, une carte à puce.

25 L'information embrouillée ne peut être désembrouillée, et donc lue par un utilisateur, qu'à hauteur des droits attribués à cet utilisateur. Les droits de chaque utilisateur sont envoyés dans des messages de gestion des droits communément notés EMM (l'abréviation EMM est issue de l'anglais « Entitlement Management Message »). Le processeur sécurisé permet de valider et d'enregistrer les droits qu'a l'utilisateur sur le service
30 délivré.

 Selon un exemple de réalisation connu de système à accès conditionnel, le prestataire de services fournit à chaque utilisateur une carte à puce et un décodeur. La sélection des messages EMM s'effectue par la mise en place d'une configuration appropriée de filtres contenus dans le
35 décodeur. Cette configuration est mise en place à partir de la lecture, par des circuits du décodeur, de données contenues dans la carte à puce. A

cette fin, l'utilisateur est amené à introduire la carte à puce dans le décodeur.

Quand les messages EMM qui correspondent à la carte à puce sont présents dans le signal que reçoit le décodeur, ils sont sélectionnés à l'aide des filtres et transférés vers la carte à puce.

Les messages EMM sont émis, de façon asynchrone, avant l'émission du service embrouillé auquel ils correspondent. Les droits utilisateur sont ainsi, par exemple, très souvent émis aux heures les plus creuses de la nuit. Par ailleurs, les droits utilisateur sont amenés à être fréquemment renouvelés sans que l'utilisateur en ait la connaissance.

Il s'ensuit qu'un utilisateur qui désire pouvoir utiliser régulièrement les services d'un prestataire se trouve pratiquement dans l'obligation de laisser en permanence la carte à puce que lui a fourni le prestataire dans le décodeur pour que le transfert des messages EMM du décodeur vers la carte à puce puisse être effectué dès que possible.

Un utilisateur qui est abonné à plusieurs prestataires de services possède autant de cartes à puce qu'il a d'abonnements. Au cas où les différents prestataires de services partagent le même décodeur, il est alors quasiment impossible, pour un utilisateur, de gérer correctement son parc de cartes à puce pour acquérir dès que possible l'ensemble des droits auxquels il peut prétendre.

L'invention ne présente pas cet inconvénient.

En effet, l'invention concerne un procédé de traitement de message (EMM) de gestion de droits qu'un utilisateur possède sur un service, le procédé comprenant:

- une étape d'introduction d'un élément de sécurité dans un décodeur,
- une étape de lecture, par des circuits du décodeur, de données contenues dans l'élément de sécurité de façon à mettre en place une configuration appropriée de filtres permettant de sélectionner le message (EMM), et
- une étape d'effacement de la configuration appropriée de filtres lors du retrait de l'élément de sécurité du décodeur. Le procédé comprend:
 - une étape de mémorisation de la configuration appropriée de filtres dans un premier circuit mémoire extérieur à l'élément de sécurité, et

- une étape permettant de remettre en place la configuration appropriée de filtres à partir de la configuration mémorisée lors de l'étape de mémorisation.

5 L'invention concerne également un décodeur de système à accès conditionnel comprenant des filtres permettant de sélectionner au moins un message (EMM) de gestion des droits qu'un utilisateur possède sur un service, des circuits permettant de lire des données contenues dans un élément de sécurité introduit dans le décodeur de façon à mettre en place une configuration appropriée de filtres pour sélectionner le message (EMM)
10 et des moyens pour effacer la configuration appropriée de filtres du fait du retrait de l'élément de sécurité du décodeur. Le décodeur comprend une zone mémoire permettant de stocker la configuration appropriée de filtres mise en place et des moyens pour remettre en place, suite à l'effacement de la configuration appropriée de filtres, la configuration appropriée de filtres
15 à partir de la configuration mémorisée.

Un avantage de l'invention est de permettre l'acquisition de droits utilisateur sans que l'élément de sécurité qui contient les données pour mettre en place la configuration de filtres permettant l'acquisition de ces droits ne soit présent dans le décodeur au moment de l'acquisition.

20 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture d'un mode de réalisation préférentiel de l'invention fait en référence aux figures 1 et 2, parmi lesquelles :

la figure 1 représente un procédé de traitement de messages (EMM) de gestion de droits utilisateur selon l'invention;
25 la figure 2 représente un décodeur et un élément de sécurité selon l'invention.

Sur toutes les figures, les mêmes références désignent les mêmes éléments.

30 La figure 1 représente un procédé de traitement de messages (EMM) de gestion de droits utilisateur selon l'invention.

Durant l'étape 1, la carte à puce qui est associée au service que désire consommer l'abonné est introduite dans le décodeur.

35 Durant l'étape 2, le décodeur lit les données contenues dans la carte à puce de façon à mettre les filtres de sélection que contient le décodeur dans une configuration permettant de sélectionner les messages EMM appropriés. Selon l'invention, l'étape 2 comprend également le stockage, dans une mémoire du décodeur, de la configuration dans laquelle

sont placés les filtres. Cette mise en mémoire s'effectue, préférentiellement, de façon simultanée avec la mise en place de la configuration des filtres.

Dans le cas où la carte à puce est encore insérée dans le décodeur lorsque les messages EMM qui lui correspondent sont reçus, le
5 transfert des droits utilisateur du décodeur vers la carte à puce s'effectue comme selon l'art antérieur (étape 3).

Comme cela est connu de l'homme de l'art, lorsque la carte à puce est retirée du décodeur, la configuration dans laquelle sont placés les filtres est effacée (étape 4). Selon l'invention, cette configuration est
10 restituée (étape 5) à l'aide des données mises en mémoire lors de l'étape 2. Le décodeur est alors avantageusement susceptible de sélectionner les messages EMM correspondant à la carte à puce sans que cette dernière ne soit insérée dans le décodeur.

Quand les messages EMM qui correspondent à une carte à puce
15 retirée sont reçus, ils sont sélectionnés et mémorisés dans une mémoire du décodeur (étape 6). Une donnée permettant de caractériser la présence des messages EMM mémorisés est également enregistrée dans la mémoire du décodeur. Cette donnée peut être, par exemple, une donnée issue de manière univoque des informations qui constituent la configuration des filtres
20 ayant permis la sélection des messages EMM.

Quand l'utilisateur insère une carte à puce dans le décodeur, une vérification est effectuée pour déterminer si des messages EMM correspondant à cette carte sont mémorisés dans le décodeur (étape 7). Une telle vérification s'effectue à l'aide de la donnée enregistrée permettant
25 de caractériser la présence des messages EMM mémorisés. A cette fin, une donnée du même type que la donnée permettant de caractériser la présence de messages EMM mémorisés est générée suite à l'introduction de la carte à puce dans le décodeur. Cette donnée du même type est alors comparée aux différentes données enregistrées permettant de caractériser la présence
30 de messages EMM mémorisés. Le résultat de la comparaison permet alors d'indiquer si des messages EMM correspondant à la carte à puce insérée sont mémorisés ou non. Si des messages EMM correspondant à la carte à puce introduite dans le décodeur sont mémorisés, ces messages EMM sont alors transférés dans la carte à puce (étape 8) où ils subissent un traitement
35 connu en soi.

La figure 2 représente un décodeur et un élément de sécurité selon l'invention.

Le décodeur 9 de système à accès conditionnel comprend :

- des filtres 11 permettant de sélectionner au moins un message EMM de gestion des droits qu'un utilisateur possède sur un service,

- des circuits 12 permettant de lire des données contenues dans un élément de sécurité 10 introduit dans le décodeur de façon à mettre en place une configuration appropriée de filtres pour sélectionner le message EMM,

- une zone mémoire 14 pour stocker la configuration appropriée de filtres mise en place,

- des moyens 13 pour effacer la configuration appropriée de filtres du fait du retrait de l'élément de sécurité 10 du décodeur, et

- des moyens 15 pour remettre en place, suite à l'effacement de la configuration appropriée de filtres, la configuration appropriée de filtres à partir de la configuration mémorisée dans la zone mémoire 14.

Selon un mode de réalisation particulier de l'invention, le décodeur comprend également des moyens (non représentés sur la figure) pour vérifier, à partir de données issues de l'élément de sécurité 10, si un message EMM est stocké dans la zone mémoire 14. Si un message EMM est stocké dans la zone mémoire 14, il est transféré du décodeur 9 vers l'élément de sécurité 10.

REVENDICATIONS

1. Procédé de traitement de message (EMM) de gestion de droits qu'un utilisateur possède sur un service, le procédé comprenant:

5 - une étape d'introduction (1) d'un élément de sécurité dans un décodeur,

 - une étape de lecture (2), par des circuits du décodeur, de données contenues dans l'élément de sécurité de façon à mettre en place une configuration appropriée de filtres permettant de sélectionner le
10 message (EMM) et,

 - une étape d'effacement (4) de la configuration appropriée lors du retrait de l'élément de sécurité du décodeur, caractérisé en ce qu'il comprend:

 - une étape (2) de mémorisation de la configuration appropriée de
15 filtres dans un premier circuit mémoire extérieur à l'élément de sécurité, et

 - une étape (5) permettant de remettre en place la configuration appropriée de filtres à partir de la configuration mémorisée lors de l'étape de mémorisation.

20 2. Procédé de traitement selon la revendication 1, caractérisé en ce qu'il comprend une étape (6) permettant de sélectionner un message (EMM) à l'aide de la configuration de filtres mise en place à l'aide de la configuration mémorisée et de mémoriser le message ainsi sélectionné dans un deuxième circuit mémoire extérieur à l'élément de sécurité.

25 3. Procédé de traitement selon la revendication 2, caractérisé en ce qu'il comprend une étape (7) permettant, à partir de données contenues dans un élément de sécurité, de vérifier si un message (EMM) est stocké dans le deuxième circuit mémoire et, si c'est le cas, une étape (8) permettant
30 de transférer le message stocké dans l'élément de sécurité.

 (4) Décodeur (9) de système à accès conditionnel comprenant:

 - des filtres (11) permettant de sélectionner au moins un message (EMM) de gestion des droits qu'un utilisateur possède sur un service,

35 - des circuits (12) permettant de lire des données contenues dans un élément de sécurité (10) introduit dans le décodeur (9) de façon à mettre

en place une configuration appropriée de filtres pour sélectionner le message (EMM),

- des moyens (13) pour effacer la configuration appropriée de filtres du fait du retrait de l'élément de sécurité (10) du décodeur, caractérisé

5 en ce qu'il comprend :

- une zone mémoire (14) pour stocker la configuration appropriée de filtres mise en place,

10 - des moyens (15) pour remettre en place, suite à l'effacement de la configuration appropriée de filtres, la configuration appropriée de filtres à partir de la configuration mémorisée dans la zone mémoire (14).

15 5. Décodeur selon la revendication 4, caractérisé en ce qu'il comprend des moyens pour vérifier, à partir de données issues de l'élément de sécurité (10), si un message (EMM) est stocké dans la zone mémoire (14).

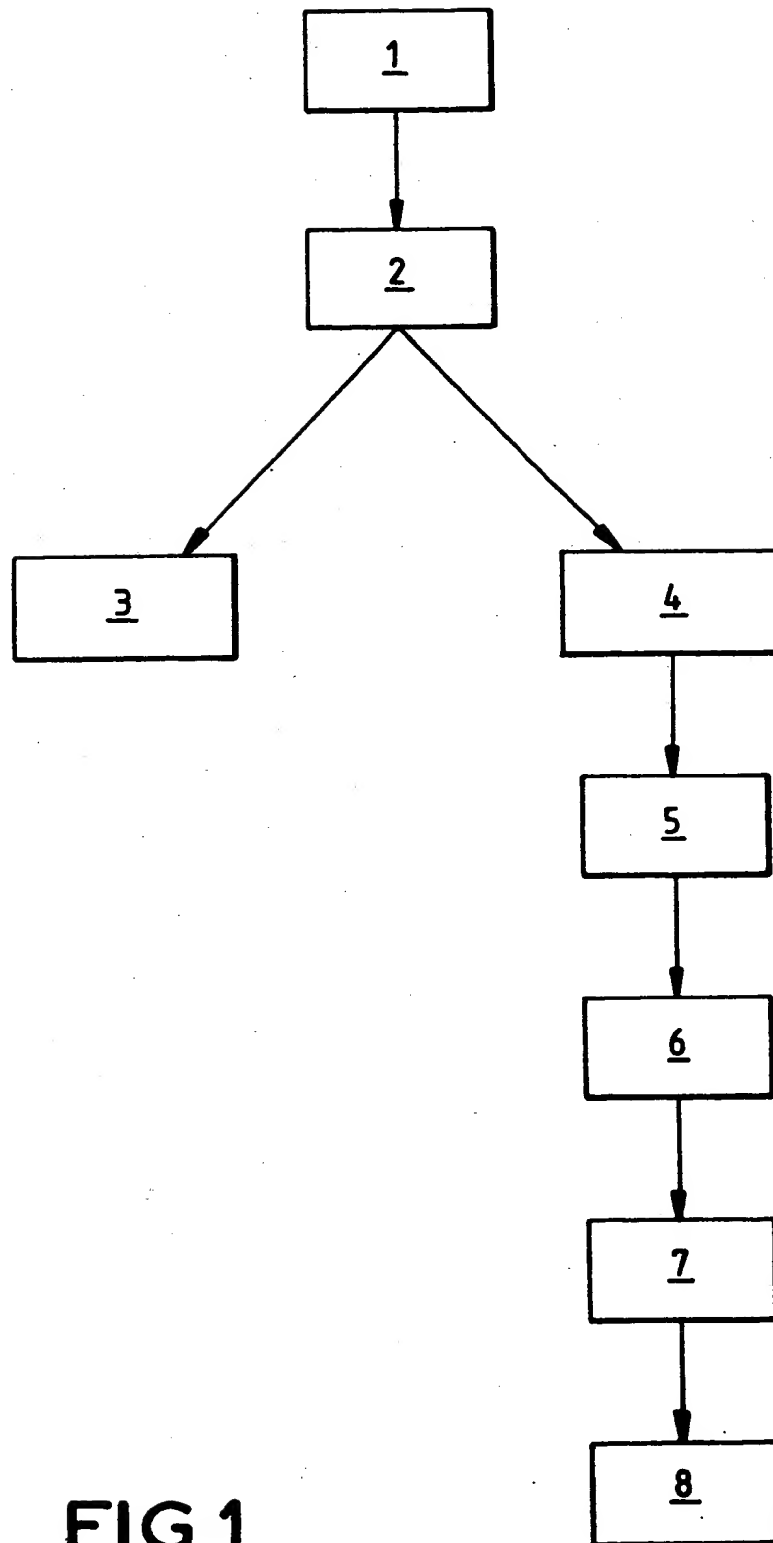


FIG.1

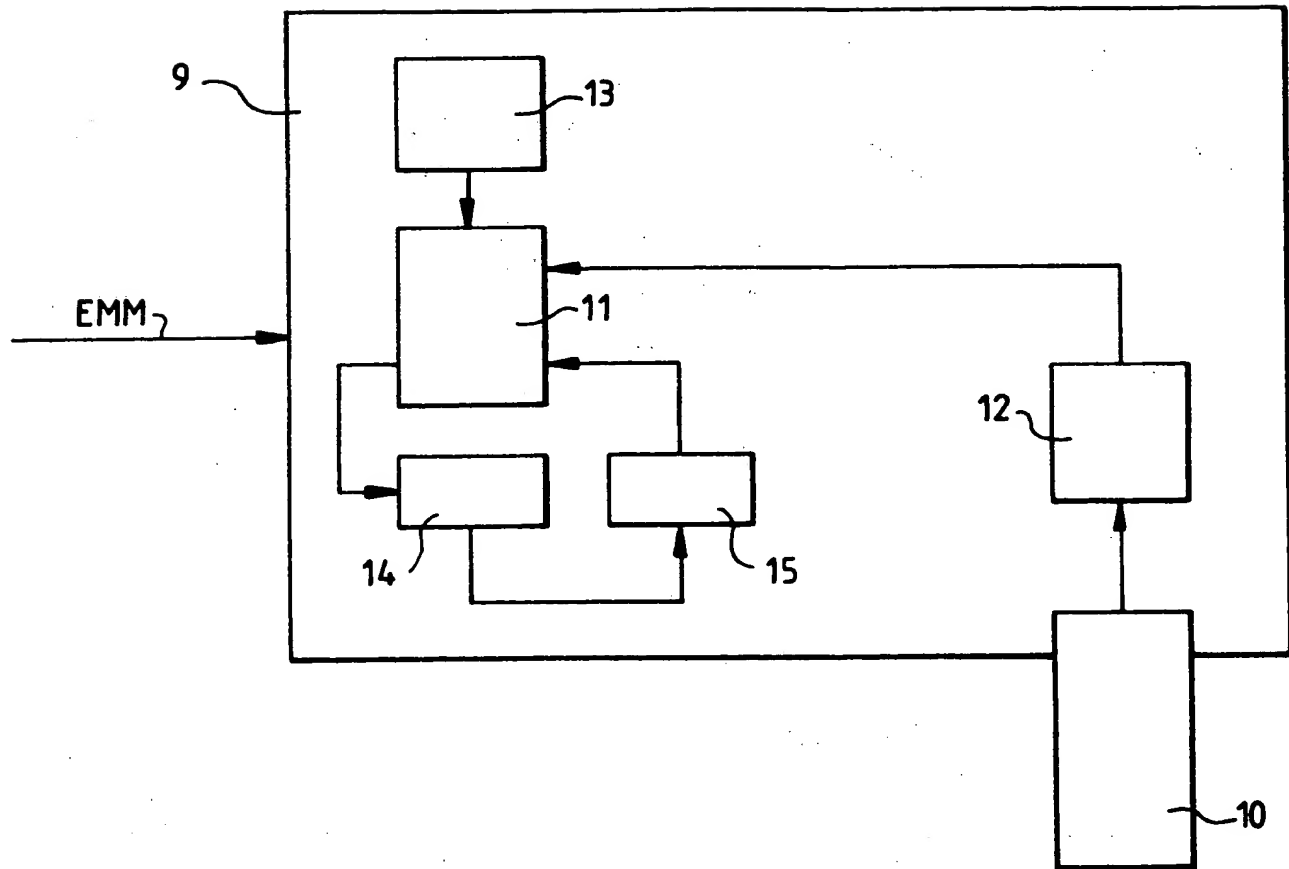


FIG. 2

THIS PAGE BLANK (USPTO)